2022 年 8 月 7 日

网络安全上升至前所未有新高度

计算机行业

事件概述：

2022 年 7 月 27 日，IBM 安全部门发布了《2022 年数据泄露成本报告》全球**数据泄露的平均成本创历史新高，达到 435 万美元。**此外根据 Canalys 数据，2020 年数据泄露事件数量泄露数量比过去 15 年的总和还多。保障我国数据安全刻不容缓！

网络安全上升至前所未有新高度

网络安全事件频发，诸如数据泄漏、勒索软件、黑客攻击等层出不穷，**全球网络安全面临严峻挑战，各国政府高度重视网络安全，**以美国、欧盟、澳大利亚为代表的国家地区纵深推进网络安全政策举措，为产业发展创造良好环境。**维护网络安全上升至国家战略，**保障关键信息基础设施的安全，对于维护国家网络安全、网络空间主权和国家安全、保障经济社会健康发展、维护公共利益和公民合法权益都具有十分重大的意义。

数据安全为数字经济保驾护航

《民法典》《数据安全法》《个人信息保护法》相继施行，**标志着我国以数据安全保障数据开发和利用产业的健康有序发展全面进入法治化轨道，**重要数据及个人信息保护成为时代需求。**从国家层面看，**保障数据安全是维护国家安全，保障数字经济健康发展，推动构筑国家竞争新优势的重要部分。**从企业层面看，**保障数据安全对于保护企业数据安全，维护企业经济利益、竞争力以及持续经营能力有着重要意义。**从个人层面看，**保障数据传输安全对于保护个人信息安全，维护个人合法权益和人身安全有着重要作用。

数据安全赋能千行百业

随着新兴技术迭代发展和数字经济的快速突进，**我国数据呈现指数级别的上涨趋势，数据安全问题日益凸显，**成为关系国家安全和经济社会发展，关系广大人民群众切身利益的重大问题。其中**数字政府是全面数字化发展的基础性、先导性工程，在促进数字经济、建设数字社会、完善数字生态中起到关键的引领作用。**网络安全厂商可以有效规避政府数据传输通道受到破坏、数据泄露、窃取、篡改等风险。**金融数据随着数字经济的创新发展呈现爆发式增长，数据采集渠道和维度多元化，数据价值密度高、应用价值大的特点愈发突出。**网络安全厂商有效规避金融数据的泄露、盗取、篡改、传输通道受到破坏、接收方责任义务确认等风险；**随着移动互联网的普及带动了数字社会总体建设步伐加快，亟需加强安全资源整合，加强API运行时安全状态防护，构建安全的数字生态系统。**

评级及分析师信息

行业评级：推荐

行业走势图

分析师：刘泽晶
邮箱：liuzj1@hx168.com.cn
SAC NO：S1120520020002

投资建议：关注数据安全厂商

重点推荐网络安全综合性龙头厂商：奇安信，以云为帆的网安龙头：深信服，地理数据安全龙头：四维图新，其他受益厂商包括安恒信息、卫士通、启明星辰、绿盟科技、天融信、美亚柏科等。

风险提示

政策推进不及预期的风险、宏观经济下滑风险、核心技术研发不及预期的风险、中美贸易摩擦升级的风险。

正文目录

图目录

1. 网络安全上升至前所未有新高度

1.1. 网络安全是不见硝烟的战场

目前，网络安全事件在世界各地频发，诸如数据泄漏、勒索软件、黑客攻击等层出不穷，**有组织、有目的的网络攻击形势愈加明显，网络安全风险持续增加，全球网络安全面临严峻挑战！**

图表 1 2022 年部分网络安全事件

公布日期	事件	内容
2022 年 2 月	**国际航港巨头遭勒索软件攻击**	全球航港巨头瑞士空港披露了一起勒索软件攻击，因 IT 基础设施与服务受到影响，导致运营被干扰。苏黎世机场透露，这波网络攻击发生在 2 月 3 日，**导致当天 22 架次航班发生轻微延误。**
2022 年 2 月	**英国外交部遭遇一起严重网络安全事件**	英国外交部承认了一起严重网络安全事件的目标。文件显示，外交和联邦事务部被迫叫来本国防务公司贝宜系统(BAE Systems)旗下的子公司应用智能(BAE Systems Applied Intelligence，主营咨询业务)来处理这一事件，**它为这项工作支付了 46.7 万英镑(约 63.3 万美元，400 万元人民币)。**
2022 年 3 月	**英伟达 1TB 内部敏感数据失窃后遭勒索**	国际芯片制造巨头英伟达证实，在上周三(2 月 23 日)遭遇了一次网络攻击，入侵者成功访问到专有信息与员工登录数据。《每日电讯报》表示，该公司经历了一场毁灭性的网络攻击，完全摧毁了内部系统。
2022 年 3 月	**乌克兰电信运营商遭遇最严重网络中断攻击**	乌克兰重要电信运营商 Ukrtelecom 遭遇“强大的”网络攻击，导致全国服务中断。专注监测互联网状态的 NetBlocks 公司称，**Ukrtelecom 可正常运行的服务“已跌至战前水平的 13%，这是自俄乌冲突以来出现的最严重的网络攻击。**
2022 年 4 月	**汽车租赁巨头全球系统中断，业务陷入混乱**	国际汽车租赁巨头 Sixt 遭到网络攻击，部分业务系统被迫中断，运营出现大量技术问题。由于系统故障，**公司的客户服务中心和部分分支机构受影响较大，业务陷入混乱**，大多数汽车预定都是通过笔和纸进行的。
2022 年 5 月	**俄罗斯胜利日，电台系统被黑**	俄罗斯总统普京在 “胜利日”阅兵式上发表讲话期间，黑客组织破坏了俄罗斯在线电视时间表页面，以显示反战信息。试图通过智能电视访问电视节目表的俄罗斯公民阅读了指责克里姆林宫的信息。俄罗斯主要电视频道、最大搜索网站 Yandex、最大视频网站 RuTube 均受到网络攻击的影响
2022 年 5 月	**俄最大银行遭到最严重 DDoS 攻击**	俄罗斯最大银行联邦储蓄银行披露，在 5 月 6 日成功击退了有史以来规模最大的 DDoS 攻击，峰值流量高达 450 GB/秒。此次攻击联邦储蓄银行主要网站的恶意流量是由一个僵尸网络所生成，**该网络包含来自美国、英国、日本和中国台湾的 27000 台被感染设备。**
2022 年 6 月	**美国医疗设备公司遭黑客攻击，**	美国医疗保健集团希尔兹就此前发生的一起网络攻击事件发表公开声明，称攻击已被遏制。**此次网络攻击导致约 200 万患者的医疗信息被泄露，包括姓名、身份证号、住址、诊断结果、保险编号等。**
2022 年 7 月	**朝鲜间谍使用 Chrome 扩展程序窃取电子邮件**	美国网络安全公司 Volexity 发现的相关恶意扩展名为 SHARPEXT，支持 Chrome、Edge 和韩国 Naver Whale 等三种基于 Chromium 的浏览器，目的是窃取 Google 和 AOL 的电子邮件。
2022 年 8 月	**中欧天然气管道公司疑遭勒索攻击导致 150GB 数据失窃。**	BlackCat 勒索软件组织声称，对上周中欧地区天然气管道与电力网络运营商 Creos Luxembourg SA 遭受的网络攻击负责，并威胁要发布总计 150 GB 大小的 18 万个被盗文件，具体涵盖合同、协议、护照、账单及电子邮件。Creos 的母公司 Encevo 目前正在调查攻击造成的损害程度。

资料来源：公开资料整理，华西证券研究所

针对网络安全事件频发、影响和规模之大，各国政府高度重视网络安全，政策方面，以美国、欧盟、澳大利亚为代表的国家地区**纵深推进网络安全政策举措，为产业发展创造良好环境。**

- **美国为保持其在未来科技领域的领先地位，持续调整其网络安全战略布局。顶层路线方面，**2021 年 3 月，白宫发布《国家安全战略临时指导方针》，将提升网络安全作为美国政府首要任务，鼓励私营部门与各级政府合作，保卫美国免受恶意网络活动侵害。2021 年 5 月，拜登签署《改进国家网络安全行政令》，**提出预防、检测、评估和处路网络安全事件是国家和经济安全的重中之重。新技术领域安全方面，**美国将人工智能、能源、量子信息科学、通信和网络技术、半导体和太空技术作为关键和新兴技术，不断强化上述领域的网络安全治理。**网络安全能力方面，**一方面美国持续推动网络安全架构演进，主要推进敦促整个国防部及其**承包商对敏感系统实施零信任。**另一方面，美国开始通过网络安全成熟度模型认证法规来加强其网络安全能力。

- **欧盟为全面提升在数字经济领域的竞争优势，维护自身的“数字主权”，多措并举促进其网络安全战略升级。一是提升网络安全核心战略地位。**2021 年 3 月提出的“2030 年欧洲数字化转型愿景”，以及欧盟新型研究与创新项目“地平线欧洲”等战略计划均将网络安全作为其发展重点板块；**二是推动出台新技术应用的安全保障措施。**主要覆盖物联网全生命周期的安全和 AI 系统的安全；**三是不断完善数据安全保障措施。**2020 年 11 月，欧盟委员会提出《数据治理法规》，以促进欧盟内部数据共享。2021 年 4 月，欧盟网络安全局发布报告《欧盟数字战略自主的网络安全研究方向》，报告确定了七个关键研究领域，以加强欧盟数字自治。

- **为维护国家安全，澳大利亚频繁部署加快网络安全战略谋化。一是强化整体网络安全战略，**2020 年 8 月，澳大利亚政府发布《2020 年网络安全战略》，依据该战略，澳政府将投资 16.7 亿美元用于建立新的网络安全和执法能力，协助行业加强自我保护，并增强社区对保护在线安全的理解。2022 年 4 月，澳大利亚政府发布《国际网络和关键技术参与战略》，用于指导澳大利亚在网络和关键技术问题上的国际参与决策，帮助其拥抱巨大创新机会并减轻或避免相关风险；**二是加速推进云安全布局，**2020年7月，澳大利亚发布《云安全指南》，为政府和整个行业安全使用云服务提供支撑；**三是重视小企业网络安全，**澳大利亚网络安全中心更新《小企业网络安全指南》，旨在帮助小型企业保护自身，免受传统的网络安全事件影响；**四是持续更新在线安全法案，**2021 年 2 月，澳大利亚更新《在线安全法案 2021》，保护网络空间中澳大利亚公民，尤其是儿童的在线安全。

图表 2 我国国家层面网络安全政策梳理

时间	法规	部分内容
2015 年 7 月 1 日	《国家安全法》	国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。
2017 年 6 月 1 日	《网络安全法》	网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力
2020 年 1 月 1 日	《密码法》	为规范密码应用和管理，促进密码事业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，提供有效法律支撑。通过立法提升密码管理科学化、规范化、法治化水平，促进我国密码事业的稳步健康发展。
2021 年 1 月 1 日	《民法典》	自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。
2021 年 3 月 11 日	《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》	第十八章提出，统筹数据开发利用、隐私保护和公共安全，加快建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范。
2021 年 9 月 1 日	《数据安全法》	第三条明确，数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。
2021 年 11 月 1 日	《个人信息保护法》	第四条明确，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

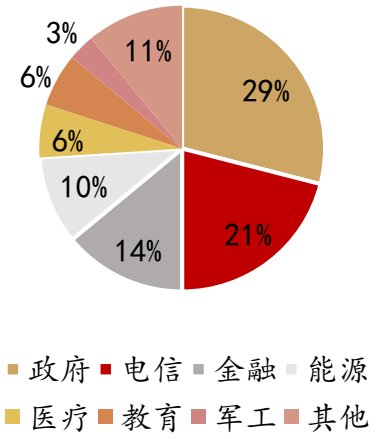
资料来源：公开资料整理，华西证券研究所

近年来，网络安全相关法律、政策持续加码，彰显我国对网络安全的高度重视程度。在国家战略引导下，我国在国家安全、网络安全、数据安全、个人信息保护、关键信息基础设施、车联网等多个领域密集出台了多项法律法规和政策文件，有效促进了网络安全领域的技术创新和应用落地，为筑牢国家网络安全屏障、推进网络强国建设提供了有力支撑。**保障关键信息基础设施的安全，对于维护国家网络安全、网络空间主权和国家安全、保障经济社会健康发展、维护公共利益和公民合法权益都具有十分重大的意义。**

图表 3 网络安全新兴领域

资料来源：华西证券研究所

图表 4 2020 年网络安全下游市场份额



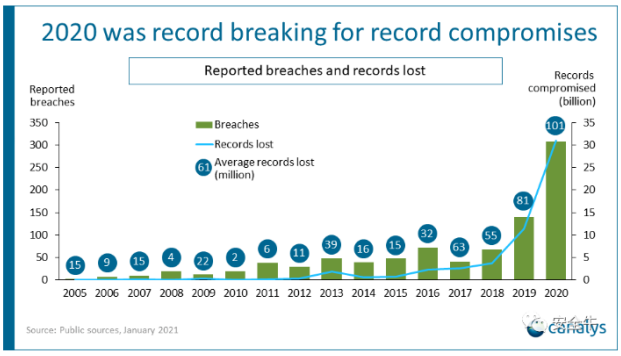
资料来源：信息安全与通信保密杂志社，华西证券研究所

此外，数据安全作为网络安全的重要枢纽部分同样被我国高度重视！《民法典》《数据安全法》《个人信息保护法》相继施行，**标志着我国以数据安全保障数据开发和利用产业的健康有序发展全面进入法治化轨道，重要数据及个人信息保护成为时代需求。**从相关法律的发布进程来看，我国数据安全领域的政策体系不断完善，基础法规架构已初步构建完成，数据安全产业将迎来发展的黄金期。

1.2. 数据安全为数字经济保驾护航

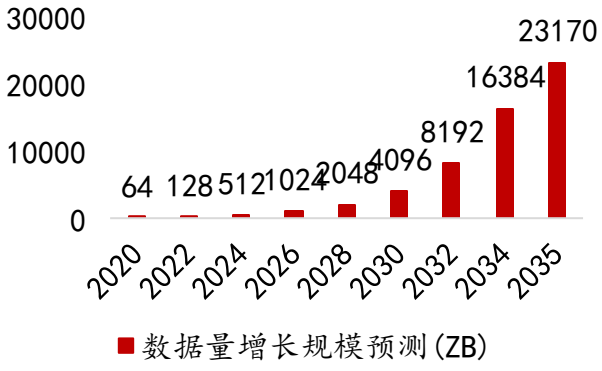
数据安全定义为通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。随着云、大、物、移、智、5G 等新兴技术迭代发展和数字经济的快速突进，**我国数据呈现指数级别的上涨趋势，数据安全问题日益凸显，成为关系国家安全和经济社会发展，关系广大人民群众切身利益的重大问题。**此外，根据 2022 年 7 月 27 日 IBM《2022 年数据泄露成本报告》，**数据泄露成本已创历史新高，平均成本可达 435 万美元。**

图表 5 2006-2020 年全球数据泄露案件数量



资料来源：Canalys、华西证券研究所

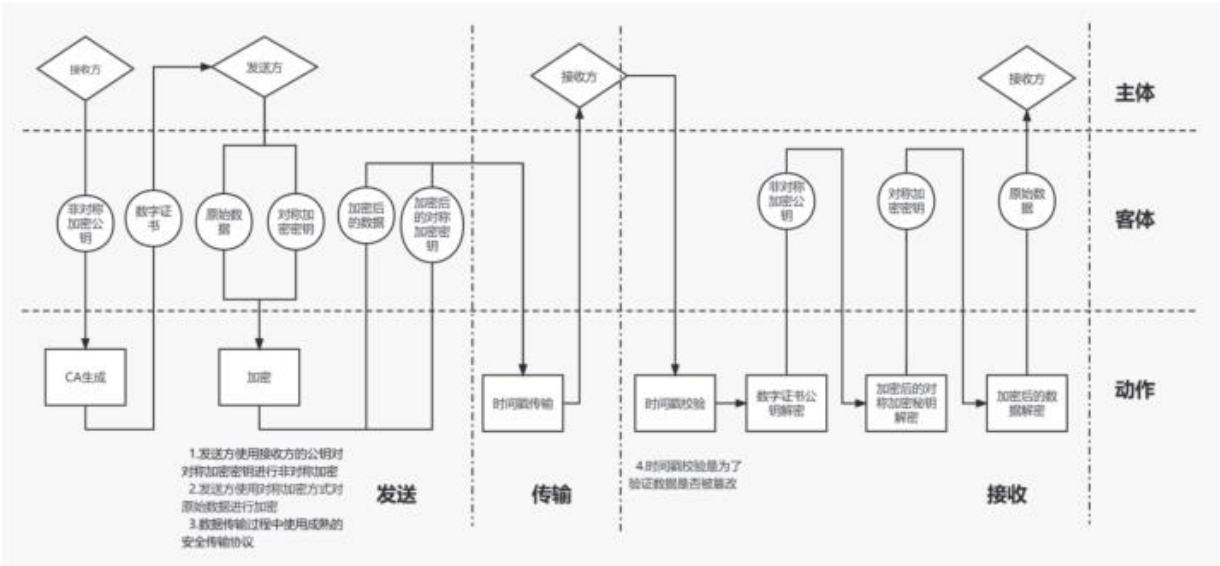
图表 6 中国数据数量规模预测



资料来源：安全牛，华西证券研究所

- **从国家层面看，保障数据安全是维护国家安全，保障数字经济健康发展，推动构筑国家竞争新优势的重要部分。对国家安全而言，**保障数据安全与国家公共服务、社会治理、经济运行、国防安全等方面密切相关；**对数字经济而言，**随着新一轮科技革命的加快推进，数据作为新型生产要素，有效促进数字基础设施发展与产业迭代升级，数字经济已成为我国经济高质量发展的新引擎，保障数据数据安全已成为我国数字经济蓬勃发展的关键所在；**对国家竞争优势而言，**发展数字技术、数字经济，加强数据治理，是全球科技革命和产业变革的先机，是新一轮国际竞争重点领域，是构筑国家竞争新优势的重要因素。
- **从企业层面看，保障数据安全对于保护企业数据安全，维护企业经济利益、竞争力以及持续经营能力有着重要意义。**在数字化转型大趋势下，数据已成为企业日常办公、生产经营、技术创新、战略发展等活动的基础，数据安全已成为数字企业健康稳定发展的基本保证。
- **从个人层面看，保障数据传输安全对于保护个人信息安全，维护个人合法权益和人身安全有着重要作用。**保障个人数据传输安全，确保个人数据在传输过程中不被篡改、破坏、泄露、窃取和非法利用，关系到个人的隐私权、决定权、知情权、人格权等多种权利，甚至关系到个人财产和人身安全。

图表 7 数据传输的框架图



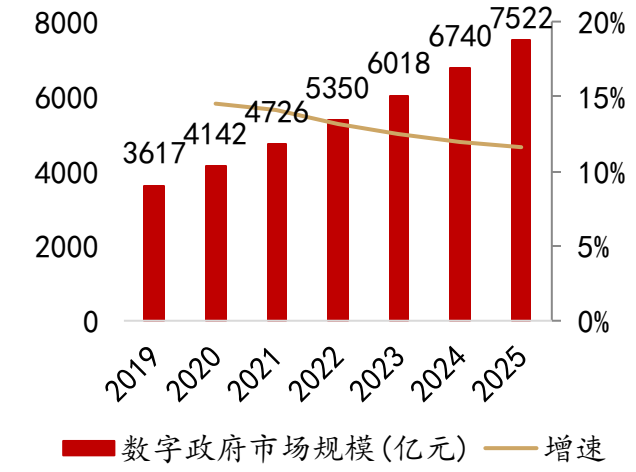
资料来源：工业和信息化部，华西证券研究所

从网络安全下游端来开，政府、电信、金融领域是网络安全的重点行业，累计占比大约占全行业的 65%。其中：

- **数字政府**

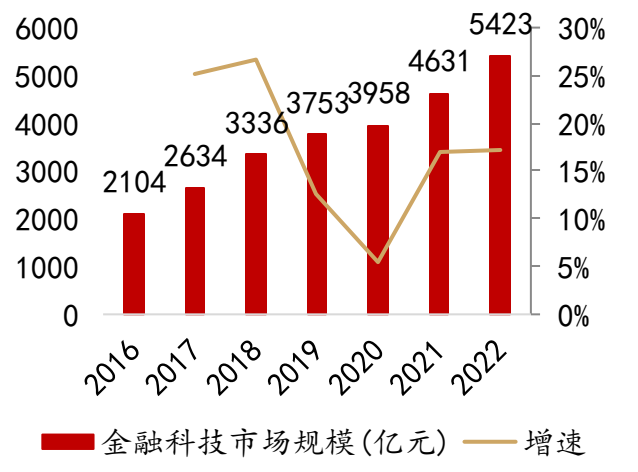
数字政府是全面数字化发展的基础性、先导性工程，在促进数字经济、建设数字社会、完善数字生态中起到关键的引领作用。**随着数字政府建设不断深入，政务数据规模快速增长，海量数据的收集、存储、使用、加工、传输、提供、公开，增加数字政府网络安全防护难度。**同时，受内外部多重因素影响，数字政府面临的网络安全威胁日益凸显，网络攻击形势愈加明显。**政府数据具有数据量庞大、数据种类繁多、涉密安全较高等特点。**

图表 8 2019-2025 年中国数字政府市场规模(亿元)



资料来源：产业信息网、华西证券研究所

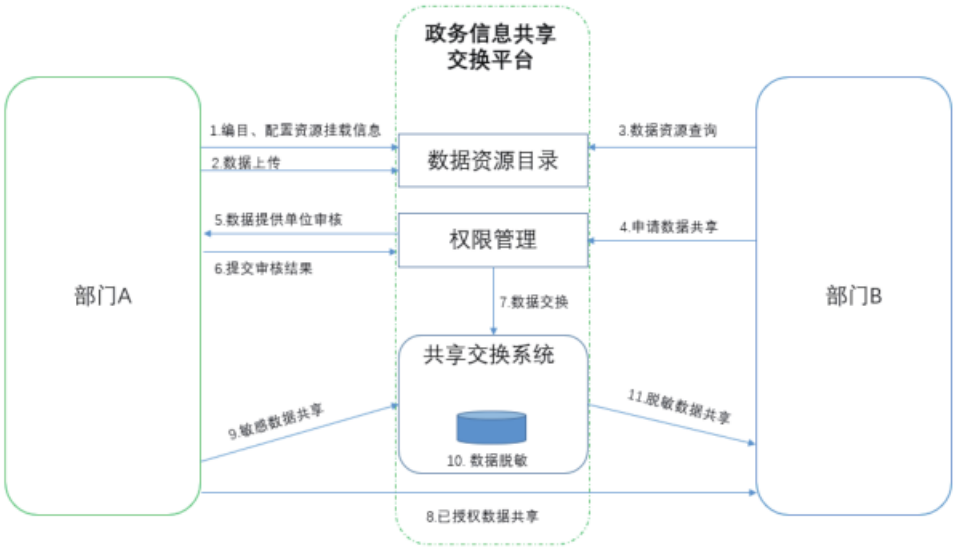
图表 9 2016-2022 中国金融科技市场规模(亿元)



资料来源：赛迪咨询，华西证券研究所

网络安全厂商在管理方面可以帮助政府、央企等建立内部网络安全管理规范、明确数据内容和加密内容等安全、合规要求。在技术方面，可以通过部署防火墙等安全设备、应对外部攻击，同时做好内部网络的安全漏洞扫描、主动防御等，可以通过 VPN 等方式帮助政府企业实现内网和外网的安全隔离；可对数据内容进行加密，并通过对加密算法、密钥强度进行优化和升级，提升数据传输过程中的安全性，并根据需要对业务数据进行脱敏处理。**网络安全厂商可以有效规避传输通道受到破坏、数据泄露、窃取、篡改等风险。**

图表 10 政务信息共享平台示意图



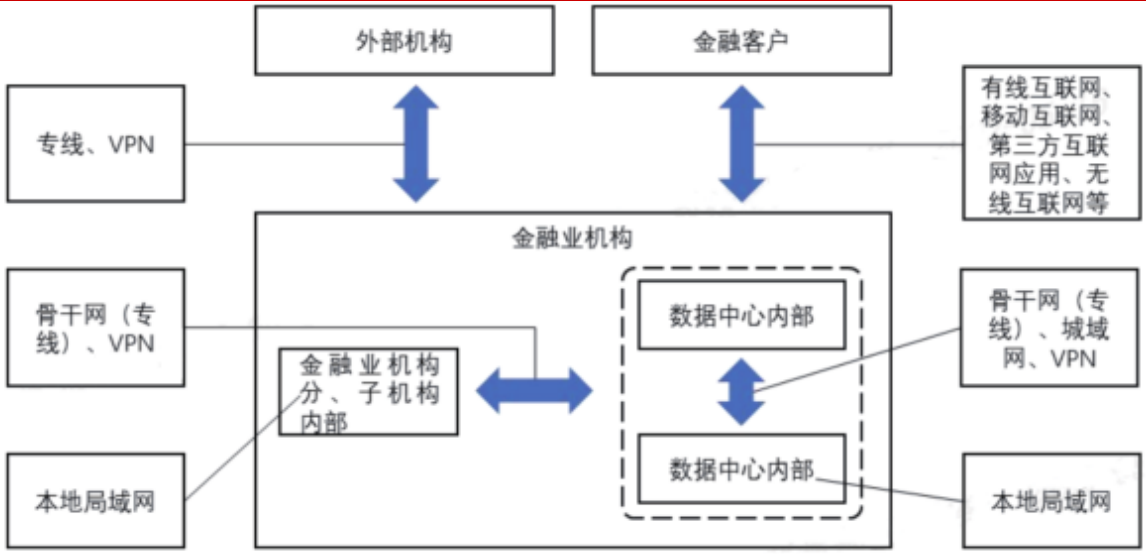
资料来源：工业和信息化部，华西证券研究所

➢ **数字金融**

近年来，随着数字经济创新发展，数字技术与金融深度融合，我国数字金融建设持续推进，为促进企业和产业数字化转型升级的提供了重要支撑。**目前数字金融的应用范围涵盖数字支付、数字货币、线上信贷、数字证券、智能理财、数字保险等新型业务形态**，主要参与机构包括银行、保险、证券、资产管理等金融

机构，以及互联网平台企业。**金融数据随着数字经济的创新发展呈现爆发式增长，数据采集渠道和维度多元化，数据价值密度高、应用价值大的特点愈发突出。金融数据的泄露、滥用、篡改等安全威胁影响重大，涉及用户个人隐私和企业商业机密，关乎国家安全和社会稳定。**加强金融数据安全能力建设既是金融机构发展的内生需求，也是行业强监管的客观要求。**金融数据具有范围较大、数量庞大、范围相对固定等特点。**

图表 11 数字金融数据安全应用场景示意图



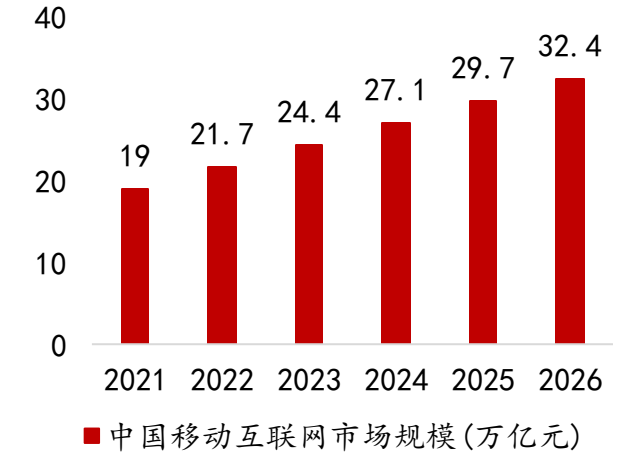
资料来源：工业和信息化部，华西证券研究所

网络安全厂商可以根据金融数据的特点，在管理方面，应对应根据数据的不同安全级别，制定和明确数据访问控制过程中的相关管理措施，建立金融信息保护制度体系及保护规范工作流程，明确工作职责。在技术方面，可通过部署防火墙等安全设备，应对外部攻击，做好内部网络的漏洞扫描、主动防御等，保证传输通道的安全，并对传输通道进行加密；同时终端应采取准入控制、终端鉴别等技术措施，防止非法或未授权终端接入。建立日常数据泄露、数据篡改、数据窃取、数据非法使用的风险监控机制，主动预防、发现和终止数据泄露异常行为。**网络安全厂商有效规避数据的泄露、盗取、篡改、传输通道受到破坏、接收方责任义务确认等风险。**

- **移动互联网**

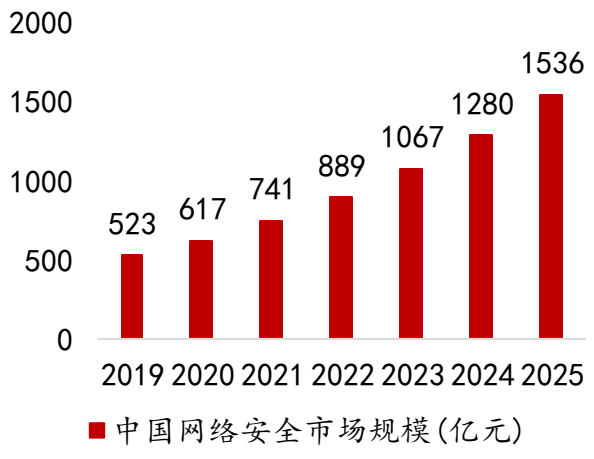
互联网已经融入经济社会生产和生活各个领域，带来新的生活方式和商业模式，教育、医疗、养老、抚幼、就业、文体、助残等重点领域数字化普惠应用发展迅速，**互联网的普及带动了数字社会总体建设步伐加快。**近年来由于敏捷性需求和微服务架构的发展，越来越多互联网应用开始通过云部署，提供云服务。API 已成为数字时代网络应用流量最重要的出入口，通过攻击 API 来破坏信息系统和窃取数据成为新风险点，**亟需加强安全资源整合，加强 API 运行时安全状态防护，构建安全的数字生态系统。**移动互联网数据具有涉及个人隐私、发送量较大、分布较广、安全建设标准不统一等特点。

图表 12 2021-2026 年中国移动互联网市场规模



资料来源：前瞻产业研究院、华西证券研究所

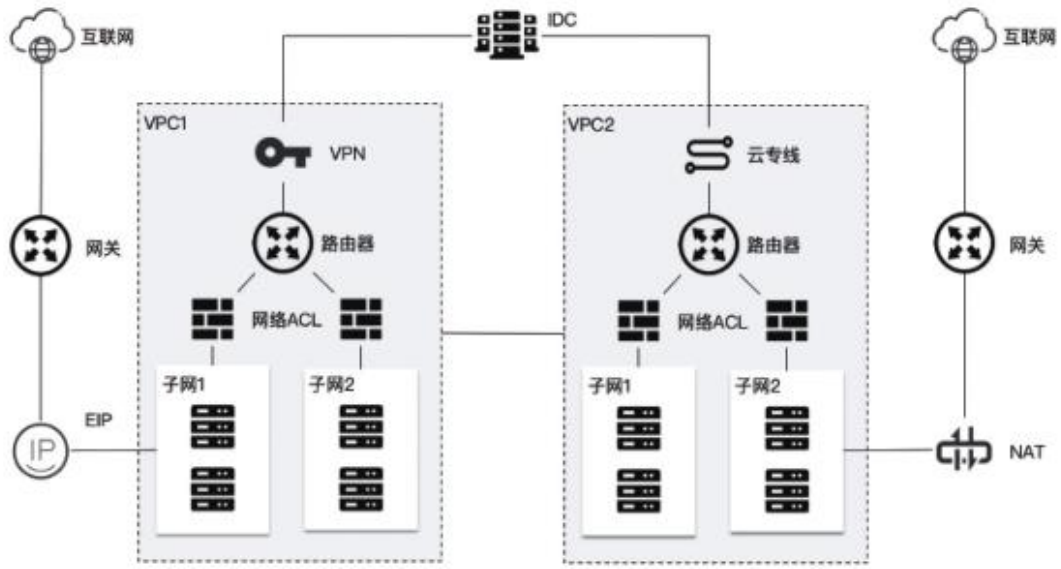
图表 13 2016-2022 中国网络安全规模及预测(亿元)



资料来源：华经产业研究院，华西证券研究所

网络安全厂商可以通过建立平台信息保护组织框架、数据安全管理平台加密方法、密钥强度等方法，有效解决**互联网的数据泄漏及遭受攻击风险、身份鉴别信息泄漏风险、客户端伪造等风险。**

图表 14 互联网安全应用场景示意图



资料来源：工业和信息化部，华西证券研究所

2. 投资建议：关注数据安全厂商

保障数据安全是维护数字经济健康发展，推动构筑国家竞争新优势的重要部分。重点推荐网络安全综合性龙头厂商：奇安信，以云为帆的网安龙头：深信服，地理数据安全龙头：四维图新，其他受益厂商包括安恒信息、卫士通、启明星辰、绿盟科技、天融信、美亚柏科等。

- **奇安信：**

奇安信是网络安全全领域全覆盖的龙头厂商具有全面的产品， 根据 2021 年 3 月安全牛发布的第八版中国网络安全行业全景图，公司的产品线覆盖 13 个一级安全领域和 94 个二级细分领域，连续多年蝉联入选全景图细分领域最多的企业；

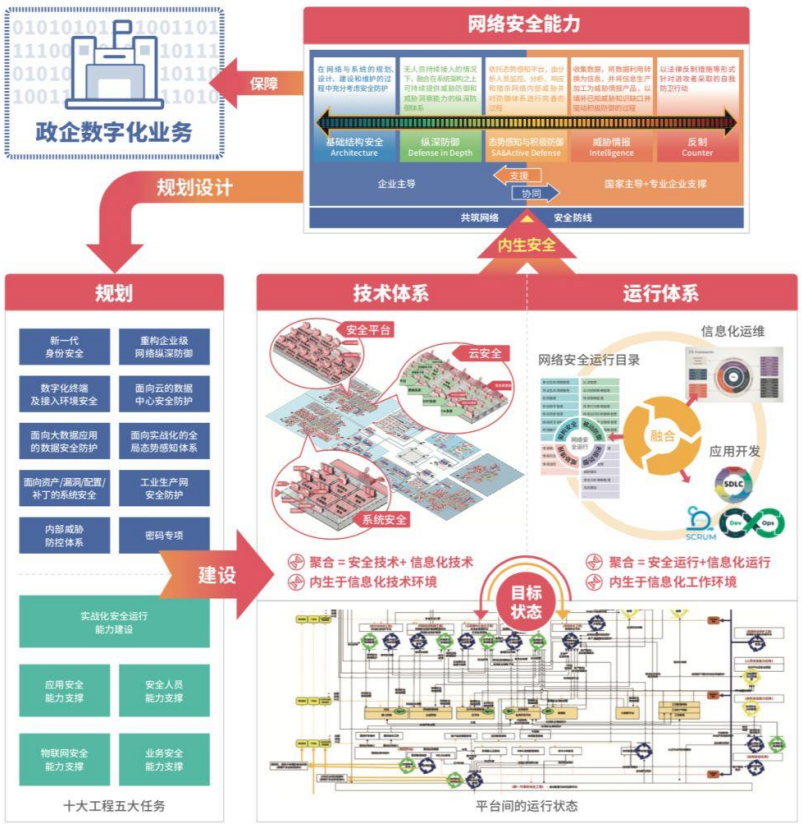
公司数据安全产品种类齐全， 包括数据安全态势感知平台、零信任数据安全产品、特权账号管理系统、运维安全管理系统、大数据安全交易沙箱、数据库安全审计与防护、数据防泄漏、源代码安全、APP 隐私合规检测平台、电子数据取证等围绕着数据全生命周期以及云、大、移、工场景下的数据安全防护品类。

公司产品行业市场地位领先，多项新赛道产品市占率第一：根据 IDC 数据，中国安全资源池、IT 安全咨询服务、托管安全服务、中国终端安全软件、中国安全分析和情报、中国政府行业 IT 安全软件市场份额位列第一，UTM、中国安全内容管理硬件分别位列第三、第二。

公司新赛道进行重点布局： 在泛终端安全、态势感知、高级威胁检测、数据隐私保护、云安全、代码安全、SD-WAN、工业互联网安全、零信任身份安全、车联网安全、物联网安全等新领域等新赛道进行布局。

公司拥有网络安全“国家队”称号，背靠中国电子，同时继承 360 底色。

图表 15 奇安信新一代网络安全框架



资料来源：奇安信官网，华西证券研究所

➢ **深信服**

深信服是“以云为帆”的网络安全公司。公司网络安全产品齐全涉及边界安全、终端安全、身份与访问安全、内容安全、云安全、安全服务等领域，核心产品及服务包括下一代防火墙、VPN、全网行为管理、SASE、零信任访问控制系统等

公司是网络安全的领军人物，旗下多款产品蝉联第一。根据 IDC 数据，VPN 产品自 2008 年至 2021 年，连续 14 年稳居国内虚拟专用网市场占有率第一；全网行为管理产品自 2009 年至 2021 年连续 13 年在安全内容管理类别中保持国内市场占有率第一；公司下一代防火墙自 2016 年至 2021 年连续 6 年在统一威胁管理类别中的国内市场占有率第二；

公司积极推进云计算业务，推出多款创新型产品包括：以虚拟化产品、超融合 HCI 产品、云计算平台 SCP、企业级分布式存储 EDS、软件定义终端桌面云 aDesk、大数据智能平台 aBDI、数据库管理平台 DMP 等

公司云产品占据一定市场地位：根据国际数据公司 IDC 数据，公司桌面云终端（原 VDI）产品 2017 年至 2020 年连续四年保持中国云终端市场占有率第二，2021 年升至第一；云桌面软件 VCC 类（桌面虚拟化、应用虚拟化）产品 2017 年至 2021 年上半年中国市场占有率保持前三；超融合 HCI 产品 2017 年至 2021 年连续五年中国市场占有率稳居前三。

公司依托在网络安全和云安全多年技术积累，为切实解决用户数据安全治理的核心痛点，公司发布多款产品及解决方案。公司 2021 年发布正式发布多云安全平台 MCSP、云主机安全保护平台 CWPP、容器安全、互联网应用和接口保护 WAAP 等多款创新产品；同时公司发布数据智能分类分级、数据安全大脑产品及综合数据安全解决方案。

图表 16 深信服云安全访问服务示意图

资料来源：深信服官网，华西证券研究所

➢ **四维图新**

四维图新作为高精度地图“国家队”，率先落地数安平台建设订单，**是车联网数据安全建设的优先受益标的。**

数据安全平台已签约四家海外龙头 OEM。去年 11 月，随着数据合规强监管的信号发出，公司凭借其“国家队”身份+地图数据处理能力的厚积累，迅速拿下多家车厂订单，相关业务放量信号明显。截至目前，四维图新已与戴姆勒、沃尔沃、福特、宝马签订数据安全相关业务订单。

数据安全业务盈利能力强，前景广阔。数安业务将实现平台建设费+订阅服务费的可持续性盈利模式，并有望横向推广至更多 OEM。另外，公司的地图和数据相关业务协同性强，拿下核心客户合作后容易进行业务的纵向延伸，进一步提升单客户价值。

图表 17 四维图业务示意图

资料来源：四维图新官网，华西证券研究所

3. 风险提示

1、政策推进不及预期的风险；

2、宏观经济下滑风险；

3、核心技术研发不及预期的风险。

4、中美贸易摩擦升级的风险。

分析师与研究助理简介

刘泽晶（首席分析师）： 2014-2015年新财富计算机行业团队第三、第五名，水晶球第三名，10年证券从业经验。

分析师承诺

作者具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，保证报告所采用的数据均来自合规渠道，分析逻辑基于作者的职业理解，通过合理判断并得出结论，力求客观、公正，结论不受任何第三方的授意、影响，特此声明。

评级说明

公司评级标准	投资评级	说明
以报告发布日后的6个月内公司股价相对上证指数的涨跌幅为基准。	买入	分析师预测在此期间股价相对强于上证指数达到或超过15%
	增持	分析师预测在此期间股价相对强于上证指数在5%—15%之间
	中性	分析师预测在此期间股价相对上证指数在-5%—5%之间
	减持	分析师预测在此期间股价相对弱于上证指数5%—15%之间
	卖出	分析师预测在此期间股价相对弱于上证指数达到或超过15%
行业评级标准		
以报告发布日后的6个月内行业指数的涨跌幅为基准。	推荐	分析师预测在此期间行业指数相对强于上证指数达到或超过10%
	中性	分析师预测在此期间行业指数相对上证指数在-10%—10%之间
	回避	分析师预测在此期间行业指数相对弱于上证指数达到或超过10%

华西证券研究所：

地址：北京市西城区太平桥大街丰汇园11号丰汇时代大厦南座5层
网址：http://www.hx168.com.cn/hxzq/hxindex.html

华西证券免责声明

华西证券股份有限公司（以下简称“本公司”）具备证券投资咨询业务资格。本报告仅供本公司签约客户使用。本公司不会因接收人收到或者经由其他渠道转发收到本报告而直接视其为本公司客户。

本报告基于本公司研究所及其研究人员认为的已经公开的资料或者研究人员的实地调研资料，但本公司对该等信息的准确性、完整性或可靠性不作任何保证。本报告所载资料、意见以及推测仅于本报告发布当日的判断，且这种判断受到研究方法、研究依据等多方面的制约。在不同时期，本公司可发出与本报告所载资料、意见及预测不一致的报告。本公司不保证本报告所含信息始终保持在最新状态。同时，本公司对本报告所含信息可在不发出通知的情形下做出修改，投资者需自行关注相应更新或修改。

在任何情况下，本报告仅提供给签约客户参考使用，任何信息或所表述的意见绝不构成对任何人的投资建议。市场有风险，投资需谨慎。投资者不应将本报告视为做出投资决策的惟一参考因素，亦不应认为本报告可以取代自己的判断。在任何情况下，本报告均未考虑到个别客户的特殊投资目标、财务状况或需求，不能作为客户进行客户买卖、认购证券或者其他金融工具的保证或邀请。在任何情况下，本公司、本公司员工或者其他关联方均不承诺投资者一定获利，不与投资者分享投资收益，也不对任何人因使用本报告而导致的任何可能损失负有任何责任。投资者因使用本公司研究报告做出的任何投资决策均是独立行为，与本公司、本公司员工及其他关联方无关。

本公司建立起信息隔离墙制度、跨墙制度来规范管理跨部门、跨关联机构之间的信息流动。务请投资者注意，在法律许可的前提下，本公司及其所属关联机构可能会持有报告中提到的公司所发行的证券或期权并进行证券或期权交易，也可能为这些公司提供或者争取提供投资银行、财务顾问或者金融产品等相关服务。在法律许可的前提下，本公司的董事、高级职员或员工可能担任本报告所提到的公司的董事。